# CASE STUDY: X-ROAD

# Starting Point

- End of 90s
- Many registries, all kept by different organizations
  - Each developed by different company
- Document exchange was done on paper
- Citizens were used as transport protocol

# Starting Point (2)

- Several bigger registries offered e-services
  - Varying quality
  - Different protocols
  - High cost of interfacing
- Data consumers were often small agencies
  - Low IT know-how
  - Low IT budget
- Confidential data, used to make high-value decisions

# Goal

- To come up with a solution that would...
  - allow effortless access to the data in state registries
  - without compromising the security of the data
  - with minimal impact to the existing systems and
  - without requiring major legal changes.

# Inception Phase

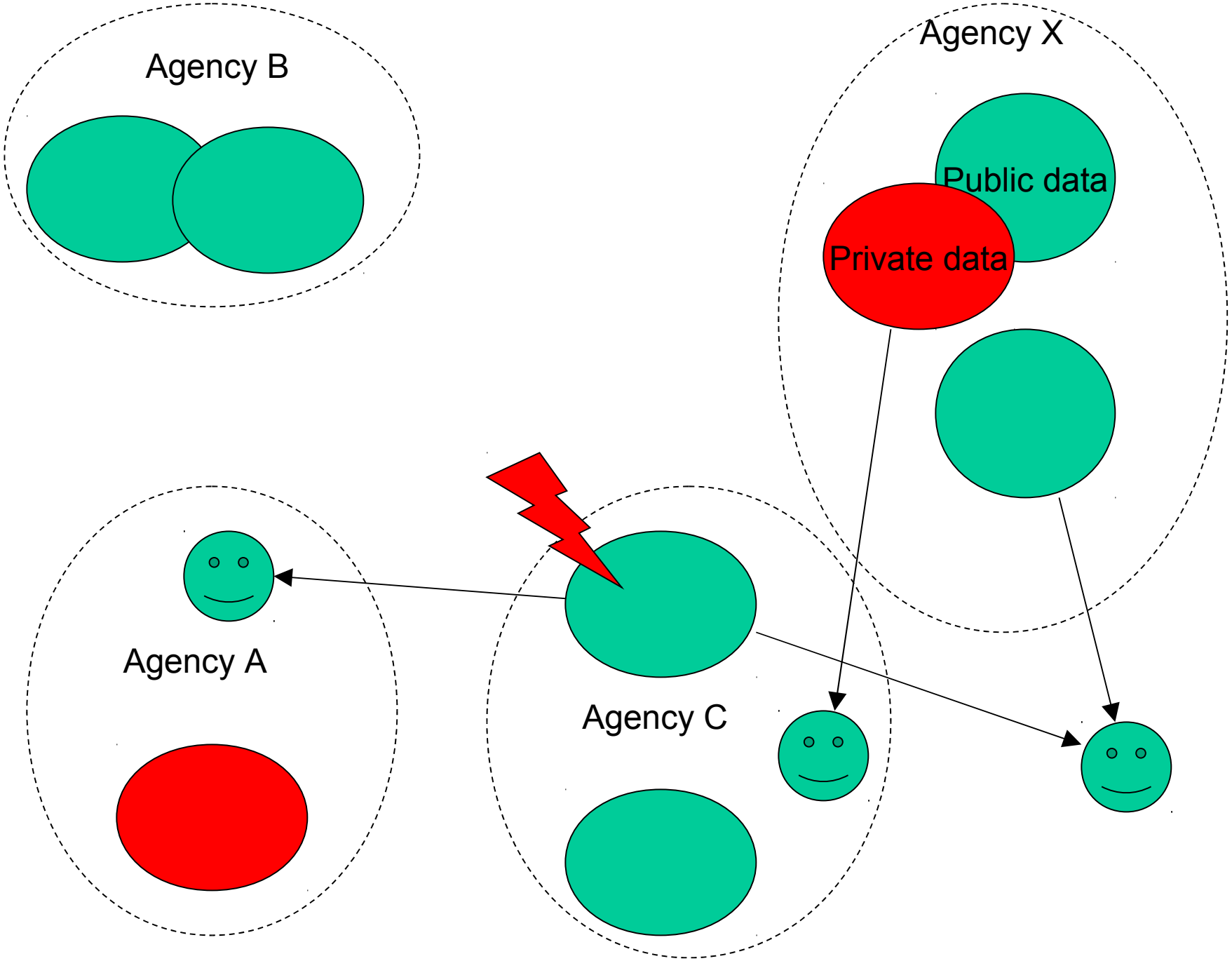
- Involved many experts from different institutions - governmental agencies, universities, IT companies
- Vision
  - Creation of the national middleware that would provide unified access to all governmental databases
  - Using web services as underlying technology

# Unification Requirements

- Unified legal framework
- Unified security measures – the initial cost of implementing the security measures will be amortized across all the state registry connections
- Unified API – all applications must be able to access all state registries in a similar way
- Unified installation and management – all installations should look like same

# Security Requirements

- Required security properties by priority:
  - Evidentiary value, authenticity, integrity
  - Availability
  - Confidentiality


Agency B
Agency X
Public data
Private data
Agency A
Agency C

# Security Requirements

- All applications required authenticity, integrity and assurance that it is possible to proof to the third party the origin of some data, received over X-Road
- In addition, it was envisioned that X-Road would be used by time-critical applications, like for performing the checks on the border. So, availability was next in the list of priorities
- And finally, the confidentiality was required in most, but not all cases

# Approach to Solution

- Develop system for highest security requirements
- That could be used by smallest organizations

- Encapsulate the complexity
- Provide functionality

# Evolution of the X-Road usage

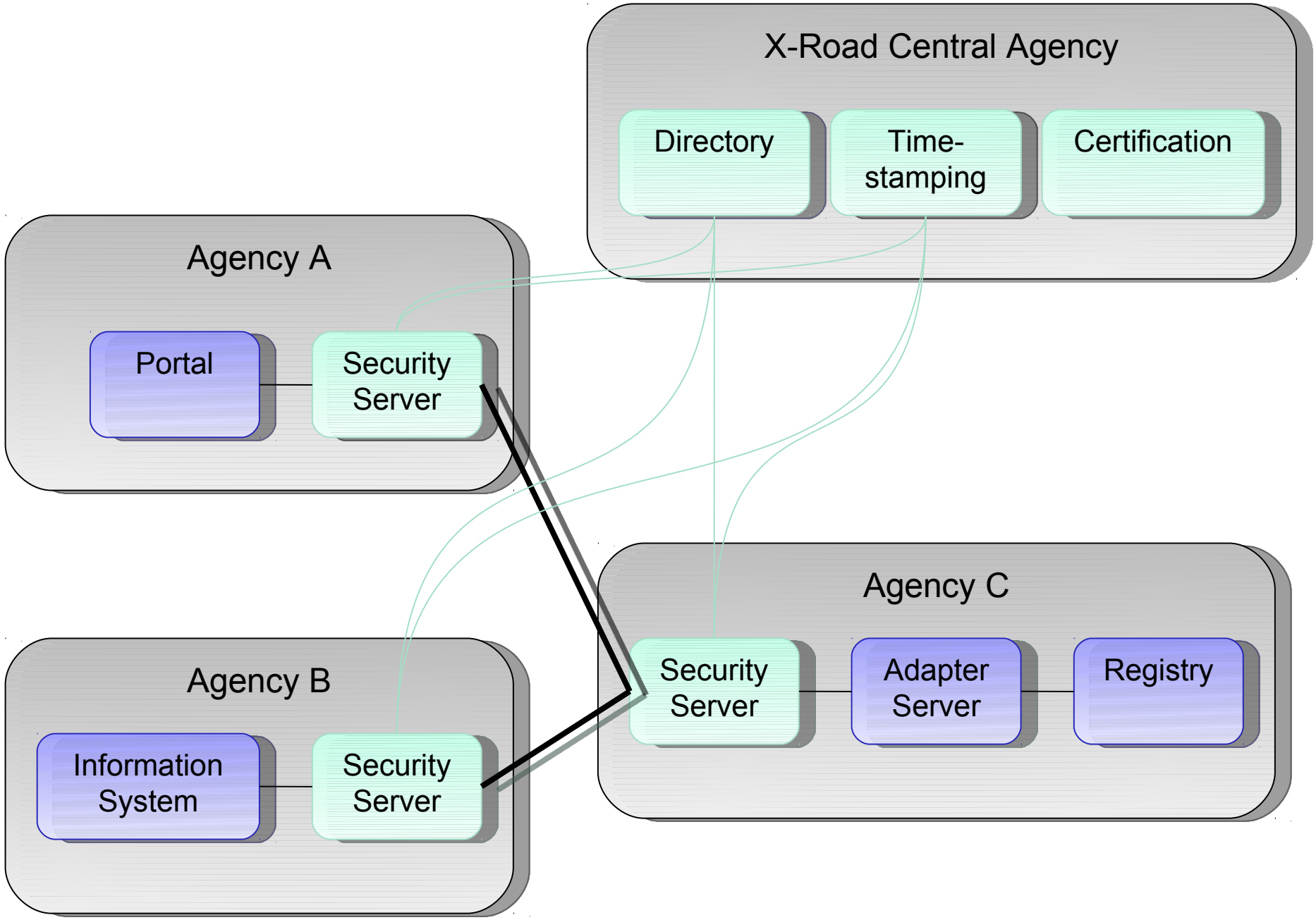
- Initially it was used just for querying the governmental databases
- Then it was used to update data in governmental databases
- Nowadays it more and more used for a generic web-services based applications
- There are no technical differences, it is just how people see and use it
- Private organizations usage of X-Road increases

# Value of the X-Road

- First of all, X-Road achieved its goal: establishing new connections between organizations is easy
- The usage of X-Road has been steadily growing
  - 57 active service providers
  - 1076 active services
  - more than 90 million transactions per year

# Components of the X-Road

- X-Road is
  - Organization
  - Legislation
  - Infrastructure
  - Technology


X-Road Central Agency
Directory
Time-stamping
Certification
Agency A
Portal
Security Server
Agency B
Information System
Security Server
Agency C
Security Server
Adapter Server
Registry

# Central Agency

- X-Road has central agency that ensures its operation
- Ensures the legal status of the X-Road and the information exchanged via it, by enforcing the stated policies
- Responsible for steering the further development of the X-Road and ensuring its consistency and integrity

# Central Services

- Certification authority
- Directory service
- Time-stamping service
- Monitoring service - detecting security breaches, collecting the statistics
- Web-based portal for citizens and smaller organizations - access to services in a simple and centralized way

# Technology: Evidentiary Value

- All outgoing messages are signed. Signing keys are certified by X-Road central agency
- All incoming messages are logged and time-stamped. X-Road central agency provides time-stamping service
- Message receiver can later prove with the help of the X-Road central agency when and by whom was the message sent

# Technology: Confidentiality

- Exchanged data is often not public or has some special access rules that must be followed
- SSL protocol is used against external attackers
- Two level access rights control mechanism is used against internal attackers:
  - Inter-organizational level
  - Intra-organizational level

# Technology: Access Control

- X-Road core deals only with inter-organizational access control, where access is granted to organization as whole
- Organization must ensure that only right people can use this service, by using whatever technical means it sees appropriate
- This obligation is enforced by service provisioning contract between the organizations

# Technology: Two Level Access Control

- Two level access control isolates the details of organizational authentication and access control mechanisms
- The impact to the existing systems was minimized
- Balanced use of technical and organizational security measures

- **Important success factor of the X-Road**

# Technology: Deployment

- Self-contained standardized monofunctional server:
  - Common PC hardware
  - Free software
  - GNU/Debian Linux based
  - Automated installer for Linux and X-Road
  - Minimal GUI
  - Built-in patching system
- Cheap and easy to install and run
- At the same time - secure

# Technology: Availability

- Distributed system, with minimal number of central services: time-stamping and secure directory
- Directory service uses Secure DNS (DNS-SEC). Well-proven DNS protocol and implementation provide robust, scalable directory service with built-in caching and redundancy. Security extensions ensure that the data cannot be tampered
- Time-stamping is used in a way that makes it non-time critical

# Technology: Availability

- Local caching DNS server ensures the availability of directory information during network outage
- Protocol supports redundant servers and load sharing
- Mechanisms against DoS attacks. Critical resources (i.e. CPU time, file handles) are shared between different clients in a fair manner

# Technology: Monitoring

- Monitoring stations for tracking the usage of the X-Road
- Central monitoring stations are run by X-Road Central Agency
  - Provides global view
- Local monitoring stations can be run by agencies running X-Road security servers
  - Provides local view

# Technology: Monitoring

- Monitoring stations collect usage statistics
- Monitoring stations provide real-time view to the system
- Monitoring stations alert the system administrators in case of anomalous activities
  - It is possible to define alerts based on the current activities and historical data
- It is also possible to integrate using existing network monitoring systems using SNMP traps

# Using X-Road

- X-Road secures web-services
- In order to use X-Road
  - Service providers are needed
  - Service consumers are needed

# Service Providers

- Must implement conforming web-services
- Adapter server
  - Simple shim for existing information systems
  - Provides web-services by using the existing API
- Information system can implement conforming web-services directly

# Service Consumers

- Ideally X-Road services are consumed by agencies integrated information system
  - Enforcement of security policies, authentication and access control of the end-users is done by existing information system
  - Maximum effectiveness - the presence of the X-Road is hidden from the users
- X-Road Portal - quick and simple way to start using X-Road

# X-Road Citizens Portal

- Provides services to all citizens
- Services that are applicable to all citizens
- Everybody can see the data about themselves
- In addition citizens can see who has looked at their personal data in registries. This helps to avoid type of misuse where "curious" officials look at the personal data